

WHAT IS CLAIMED IS:

- 1 1. A method for ensuring a secure programming environment for a computer system
2 comprising the steps:
3 modifying a processor of said computer system to incorporate an S-latch, a first
4 state of said S-latch setting said processor in a secure state and a second state of said S-
5 latch setting said processor in a non-secure state;
6 writing a security code in an NVRAM coupled to said computer system;
7 reading said security code from said NVRAM;
8 setting said first and second state of said S-latch in response to states of said
9 security code; and
10 not accepting processor commands from an In Circuit Emulator (ICE) unit
11 coupled to said computer system when said S-latch is in said first state and accepting
12 processor commands from said ICE unit when said S-latch is in said second state.
- 1 2. The method of claim 1, wherein said security code is read by boot block code
2 within a Basic Input Output System (BIOS) code of said computer system.
- 1 3. The method of claim 2, wherein said S-latch is set by said boot block code in
2 response to reading said security code.
- 3 4. The method of claim 2, wherein said boot block code is a first code executed on
4 each power up or system reset of said computer system.
- 1 5. The method of claim 1, wherein said security code is encrypted when written into
2 said NVRAM unit.

3 6. The method of claim 1, wherein said security code is password protected when
4 written into said NVRAM unit.

1 7. The method of claim 2, wherein said BIOS code is executed if said boot block
2 code is able to authenticate said security code and said boot block code is able to write
3 to said S-latch if said security code corresponds to setting said first state of said S-latch.

1 8. The method of claim 2, wherein said BIOS code is not executed if said boot block
2 code is not able to authenticate said security code.

1 9. The method of claim 2, wherein said BIOS code is not executed if said boot block
2 code is able to authenticate said security code and said boot block code is not able to set
3 a state of said S-latch.

1 10. The method of claim 1, wherein said ICE unit is coupled to said computer system
2 on a system bus of said computer system.

1 11. The method of claim 1, wherein said ICE unit is coupled to said computer system
2 on a JTAG scan chain bus.

1 12. The method of claim 1, wherein said ICE unit is coupled to said computer system
2 in place of said modified processor.

1 13. The method of claim 1, wherein a default said S-latch in said computer system
2 is set to a non-secure state.

1 14. A computer system comprising:
2 a central processing unit (CPU);
3 a random access memory (RAM);
4 non-volatile RAM (NVRAM);
5 a communications adapter coupled to a communication network;
6 an I/O adapter;
7 a bus system coupling said CPU to said NVRAM, said communications adapter,
8 said I/O adapter, and said RAM, wherein said CPU further comprises:
9 a modified processor with an S-latch, a first state of said S-latch setting said
10 modified processor in a secure state and a second state of said S-latch setting said
11 modified processor in a non-secure state;
12 circuitry operable to receive and write a security code in said NVRAM;
13 circuitry operable to read said security code from said NVRAM; and
14 circuitry operable to set said first and second state of said S-latch in response to
15 states of said security code;
16 wherein said modified processor accepts commands from an In Circuit Emulator
17 (ICE) unit coupled to said computer system when said S-latch is in said second state and
18 does not accept processor commands from said ICE unit when said S-latch is in said first
19 state.

1 15. The computer system of claim 14, wherein said security code is read by boot
2 block circuitry within Basic Input Output System (BIOS) circuitry of said computer
3 system.

1 16. The computer system of claim 15, wherein said S-latch is set by said boot block
2 circuitry in response to reading said security code.

3 17. The computer system of claim 15, wherein said boot block circuitry reads said
4 security code as a first operation on each power up or system reset of said computer
5 system.

1 18. The computer system of claim 14, wherein said security code is encrypted when
2 written into said NVRAM unit.

1 19. The computer system of claim 14, wherein said security code is pass word
2 protected when written into said NVRAM unit.

1 20. The computer system of claim 15, wherein said BIOS circuitry is enabled if said
2 boot block code is able to authenticate said security code and said boot block code is able
3 to write to said S-latch if said security code corresponds to setting said first state of said
4 S-latch.

1 21. The computer system of claim 15, wherein said BIOS circuitry is disabled if said
2 boot block is not able to authenticate said security code.

1 22. The computer system of claim 15, wherein said BIOS circuitry is disabled if said
2 boot block circuitry is not able to set said S-latch into a state.

1 23. The computer system of claim 14, wherein said ICE unit is coupled to said
2 computer system on a system bus of said computer system.

1 24. The computer system of claim 14, wherein said ICE unit is coupled to said
2 computer system on a JTAG scan chain bus.

3 25. The computer system of claim 14, wherein said ICE unit is coupled to said
4 computer system in place of said modified processor.

1 26. The computer system of claim 14, wherein a default said S-latch in said computer
2 system is set to a non-secure state.